IN THE CLAIMS

1.(Currently amended) A data processing apparatus for generating a verifying value for verifying an individual contents data to be stored in a memory device, storing said verified value in said memory device in correspondence with said contents data, and checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to said verifying value, comprising:

a ciphering unit for generating said verifying value; and

one or more keys for use by said ciphering unit to generate said verifying value;

whereby said processing apparatus is operable to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device; and

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

2.(Previously Presented) The data processing apparatus according to Claim 1, wherein

said data processing apparatus is operable to compute an updated verifying value for one of said categories of contents data and compare said updated verifying value to the corresponding previously generated verifying value to determine whether or not there has been any tampering with the contents data corresponding to said category.

3.(Previsously Presented) The data processing apparatus according to Claim 1, wherein said plurality of categories respectively correspond to a plurality of directories; and

said verifying value is generated to deal with an assemblage of contents data individually corresponding to said plurality of directories.

4. (Previously Presented) The data processing apparatus according to Claim 1, wherein

said memory device comprises a flash memory; and

said verifying values per category are stored in a domain preset as a utilization inhibited block in said flash memory.

5. (Canceled)

6. (Previously Presented) The data processing apparatus according to Claim 1, wherein

said categories are preset and each corresponds to a node in a hierarchical structure of categories.

7. (Previously Presented) The data processing apparatus according to Claim 1, wherein

said verifying values are individually generated based on message authentication codes which are generated by applying the Data Encryption Standard to a partial data message constituting a contents related data to be subject to verification via said verifying values.

8. (Currently amended) A data processing apparatus which generates and stores message authentication codes functioning themselves as the data for probing the act of tampering with contents data or header data stored in a memory device, comprising:

a ciphering unit for generating a verifying value; and

one or more keys for use by said ciphering unit to generate one or more message authentication codes on which said verifying value is based;

whereby said processing apparatus is operable to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device; and

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

9. (Currently Amended) A data processing method, comprising the steps of:

using one or more keys to generate ~~generating~~ a verifying value for each category of a plurality of categories of contents data stored in a memory device, each said verifying value to be used for verifying an individual contents data stored in ~~a~~ said memory device,

storing each said verifying values in said memory device in correspondence with a respective one of said individual contents data, and

checking for the actual occurrence of an act of tampering with said contents data by referring to one or more of said verifying values;

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

10. (Previously Presented) The data processing method according to Claim 9, wherein said step of checking comprises the steps of computing an updated verifying value for one of said categories of contents data and comparing said updated verifying value to the corresponding previously generated verifying value to determine whether or not there has been any tampering with the contents data corresponding to said category.

11. (Previously Presented) The data processing method according to Claim 9, wherein

said plurality of categories respectively correspond to a plurality of directories; and

said verifying value is generated to deal with an assemblage of contents data individually corresponding to said plurality of directories.

12. (Previously Presented) The data processing method according to Claim 9, wherein

said memory device comprises a flash memory; and

said verifying values per category are stored in a domain preset as a utilization inhibited block in said flash memory.

13. (Canceled)

14. (Previously Presented) The data processing method according to Claim 9, wherein

said categories are preset and each corresponds to a node in a hierarchical structure of categories.

15. (Previously Presented) The data processing method according to Claim 9, wherein

said verifying values are individually generated based on message authentication codes which are generated by applying the Data Encryption Standard to a partial data message constituting a contents related data to be subject to verification via said verifying values.

16. (Previously Presented) The data processing method according to Claim 15, wherein said step of generating a verifying value includes generating one or more message authentication codes on which said verifying value is based.

17. (Currently Amended) A data processing method which generates and stores message authentication codes functioning as data for probing for an act of tampering with contents data or header data stored in a memory device, comprising the steps of:

performing ciphering according to one or more keys to generate said message authentication codes; and

using said message authentication codes to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device; and

using said verifying values for probing for an act of tampering with the contents data or header data stored in the memory device;

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

18.(Currently Amended) A recording medium recorded with a computer program executable by a computer for performing a data processing method, the method comprising the steps of:

using one or more keys to generate ~~generating~~ a verifying value for each category of a plurality of categories of contents data stored in a memory device, each verifying value to be used for verifying an individual contents data stored in said memory device,

storing said verifying values in said memory device in correspondence with said contents data, and

checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to one or more of said verifying values;

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

19.(Currently Amended) A data processing apparatus comprising:

a memory device; and

a device for (a) using one or more keys to generate ~~generating~~ a verifying value for verifying an individual contents data to be stored in the memory device, (b) storing the verifying value in the memory device in correspondence with the individual contents data, and (c) checking for the occurrence of an act of tampering with said individual contents data by referring to said verifying value;

wherein said processing apparatus is operable to generate a verifying value for each category of a plurality of categories of contents data stored in the memory device; and

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

20. (Previously Presented) The data processing apparatus of claim 19, wherein the device computes the verifying value based on data from the individual contents data and then compares the computed verifying value to a previously stored verifying value, and finally utilizes the individual contents data solely in the case in which both values are identified to be coincident with each other.

21. (Previously Presented) The data processing apparatus of claim 19, wherein said plurality of categories respectively correspond to a plurality of directories; and wherein the verifying value is generated to deal with an assemblage of contents data individually corresponding to the plurality of directories.

22. (Previously Presented) The data processing apparatus of claim 19, wherein the memory device comprises a flash memory; and the verifying value associated with the category is stored in a domain preset as a utilization inhibited block in said flash memory.

23. (Canceled)

24.(Previously Presented) The data processing apparatus of claim 19, wherein said plurality of categories are preset and each corresponds to a node in a hierarchical structure of categories.

25.(Previously Presented) The data processing apparatus of claim 19, wherein the verifying value is individually generated based on a message authentication code, which is generated by applying a Data Encryption Standard to a partial data message comprising data to be subject to verification via said verifying value.

26.(Currently Amended) A data processing apparatus comprising:

a memory device for storing contents data; and

a device for (a) generating and storing message authentication codes functioning as data for probing for an act of tampering with the stored contents data, (b) using one or more keys to generate ~~generating~~ a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and (c) renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes;

whereby said processing apparatus is operable to use one or more of said message authentication codes to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device; and

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

27. (Currently Amended) A method for use in a data processing apparatus, the method comprising the steps of:

~~initially~~ using one or more keys to generate ~~generating~~ a verifying value for each category of a plurality of categories of contents data stored in a memory device, each verifying value to be used for verifying an individual contents data stored in ~~a~~ said memory device;

storing the verifying value in the memory device in correspondence with the contents data; and

checking to probe for the occurrence of an act of tampering with said contents data by referring to said verifying value;

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

28. (Previously Presented) The method of claim 27, further comprising the steps of:

computing the verifying value based on data from the individual contents data; and

comparing the computed verifying value to a previously stored verifying value;

using the individual contents data solely in the case in which both values are identified to be coincident with each other.

29. (Previously Presented) The method of claim 27, wherein said plurality of categories respectively correspond to a plurality of directories; and wherein the verifying value is generated to deal with an assemblage of contents data individually corresponding to the plurality of directories.

30. (Previously presented) The method of claim 27, wherein the memory device comprises a flash memory; and the verifying value associated with the category is stored in a domain preset as a utilization inhibited block in said flash memory.

31. (Canceled)

32. (Previously Presented) The method of claim 27, wherein said plurality of categories are preset and each corresponds to a node in a hierarchical structure of categories.

33. (Previously Presented) The method of claim 27, wherein the verifying value is individually generated based on a message authentication code, which is generated by applying a Data Encryption Standard to a partial data message comprising data to be subject to verification via said verifying value.

34. (Previously Presented) The method of claim 27 further comprising the steps of:

generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes.

35. (Currently Amended) A method for use in a data processing apparatus, the method comprising the steps of:

using one or more keys to generate ~~generating~~ a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and

renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes; and

using one or more of said message authentication codes to generate a verifying value for each category of a plurality of categories of contents data stored in a memory of said processing apparatus;

wherein said verifying values are used in an operation that provides an indication of whether or not there has been tampering with said contents data; and

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.

36. (Currently Amended) A computer-readable medium for storing computer-executable software code, the code comprising:

code for using one or more keys to generate ~~initially~~ ~~generating~~ a verifying value for each category of a plurality of categories of contents data stored in a memory device, each verifying value to be used for verifying an individual contents data to be stored in ~~a~~ said memory device;

code for storing the verifying value in the memory device in correspondence with the contents data; and

code for checking to probe for the occurrence of an act of tampering with said contents data by referring to said verifying value;

whereby said keys are arranged in a hierarchical structure having a plurality of levels, said memory device is associated with a device level of said structure, and said memory device stores, in unencrypted form, at least one key corresponding to a level of said structure above said device level.